

**IN THE CLAIMS:**

Please amend claims 1 and 32 as follows:

Sub  
CV  
BT  
1. (Currently Amended) A system for managing one or more storage devices in a computing system having a client connected to a server over a network, the system comprising:

at least one agent operating on the server, the agent communicating with a storage device;

an agent manager operating on the server, the agent manager tracking the agents;

an applet operating on the client and adapted to provide a user interface for managing the storage devices, the applet communicating with the agent over the network to obtain information about the storage devices; and

an applet manager operating on the client, the applet manager invoking and communicating with the applet.

wherein the agent manager registers an agent upon instantiation, receives requests from clients to establish a communication link with the agent, authenticates the client, and passes connection information to an authenticated client to enable the client to establish a direct communication connection with the agent.

2. (Original) The system of claim 1, further comprising:

a firmware file adapted to be transferred from the applet over the network to an agent.

3. (Original) The system of claim 2, wherein the firmware file includes a copy of the firmware with a data header embedded therewith.

4. (Original) The system of claim 2, wherein the applet transfers over the network the firmware file to the agent so that the firmware can be downloaded to the storage device.

5. (Original) The system of claim 4, wherein the applet instructs the agent to download the firmware to the storage device, and in response, the agent initiates a process for downloading the firmware to the storage device.

6. (Original) The system of claim 3, wherein the firmware file further includes data corresponding to the version of the firmware.

7. (Original) The system of claim 3, wherein the firmware file further includes data corresponding to identification of the storage device type.

8. (Original) The system of claim 3, wherein the firmware file further includes data corresponding to an encrypted password.

9. (Original) The system of claim 3, wherein each agent is comprised of a first layer communicating with the storage devices, a second layer having data corresponding to the object representation of the storage device, and a third layer adapted to certain command data for controlling an operation of the storage device.

10. (Original) The system of claim 9, wherein each agent further comprises a fourth layer adapted to communicate with the network.

11. (Original) The system of claim 10, wherein the fourth layer is adapted to support multiple protocols.

12. (Original) The system of claim 9, wherein the third layer is adapted to support multiple command sets.

13. (Original) The system of claim 3, wherein the data header is adapted to include one or more data sets corresponding to storage devices having different characteristics.

14. (Original) The system of claim 3, wherein the data header is adapted for downloading firmware of variable segment size.

15. (Original) The system of claim 1, wherein the agent registers with the agent manager after the agent is created.

16. (Original) The system of claim 15, wherein the applet communicates with the agent manager using a single port.

17. (Original) The system of claim 1, wherein the applet communicates with the agent through the agent manager.

18. (Original) The system of claim 1, wherein the applet has an adapter module, a device module, and a subsystem module.

19. (Original) The system of claim 18, further comprising:  
a device interface object in communications with the device module and the adapter module;

at least one subsystem device object in communications with the subsystem module and the adapter module;

an adapter object in communications with the subsystem module and the adapter module; and

a network object in communications with the subsystem module and the server.

20. (Original) The system of claim 3, wherein the applet includes one or more objects instantiated in the client.

21. (Original) The system of claim 3, wherein the applet has a module for interfacing with the object representation of the storage device.

22. (Original) The system of claim 15, wherein the agent manager passes identification information about the agents to the applet manager after the agent registers with the agent manager.

23. (Original) The system of claim 1, wherein before the applet can communicate with the agent, the applet provides said identification information to the agent manager, and the agent manager authenticates the applet.

24. (Original) The system of claim 1, wherein the agent manager polls the agents to determine if the agents are operating on the server.

25. (Original) The system of claim 3, further comprising:  
a storage management database maintained by the agent containing data about the storage devices.

26. (Original) The system of claim 25, wherein the applet can access the data about the storage devices by generating a request to said agent.

27. (Original) The system of claim 25, wherein the applet can access the data about the storage devices by generating a request to said agent manager.

28. (Original) The system of claim 3, wherein said agent manager provides a first level of security, and said applet manager provides a second level of security.

29. (Original) The system of claim 3, wherein said agent transmits an event notification message to an asynchronous event service in response to a status change of said storage device.

30. (Original) The system of claim 29, wherein the asynchronous event service is capable of becoming a primary asynchronous event service when an existing primary asynchronous event service fails.

31. (Original) The system of claim 3, wherein said agent is adapted to download the firmware file to multiple storage devices simultaneously.

32. (Currently Amended) A method for downloading firmware to at least one of a plurality of storage devices of a computing system having at least one client connected to a server, the method comprising the steps of:

- instantiating an agent on a server;
- registering the agent with an agent manager on the server;
- creating, at a client, a firmware file, including a copy of the firmware with a data header embedded therewith;
- receiving, at the agent manager a request from a client to download firmware to at least one storage device;
- authenticating the client at the agent manager;
- passing connection information to the authenticated client to enable the client to establish a direct communication connection with an agent on the server;
- generating a list of one or more storage devices for receiving the firmware file;
- determining whether the storage devices on the list are updatable, and removing the devices that are not updatable from the list of storage devices for receiving the firmware file;
- transferring the firmware file and the list of storage devices from the client to the an agent instantiated on the server;
- instructing an agent operating on the server to download the firmware to the devices on the list of storage devices; and
- responsive to the instructing step, initiating a thread for downloading the firmware to the devices on the list of storage devices.

33. (Original) The method of claim 32, wherein the creating a firmware file step further comprises:

- including, in the firmware file, data corresponding to the version of the firmware; and
- including, in the firmware file, data corresponding to identification of the storage device type.

Cl  
st  
cont

Cont

34. (Original) The method of claim 32, wherein the creating a firmware file step further comprises:

including, in the image file, data corresponding to an encrypted password associated with the firmware.

---